Environmental Management Consolidated Business Center (EMCBC)

Subject: Digital Authorization in Applications and Databases

Policy Statement APPROVED: **(Signature on File)**
EMCBC Director
ISSUED BY: Office of Information Resource Management

1. POLICY

The purpose of this policy is to define the requirements for digital authorization within enterprise applications developed and/or maintained by Environmental Management Consolidated Business Center (EMCBC).

2. SCOPE

This policy applies to all EMCBC developed and maintained applications and databases that are part of general development activities, within the scope of IMP-8308-03, Software Application Development and Management, (Ref. 4.2.2). This policy does not apply to or affect the use of Entrust software or the DOE maintained Public Key Infrastructure (PKI).

3. APPLICABILITY

This EMCBC policy applies to all Federal and contractor entities that develop or maintain applications or databases in which electronic input is used to authorize or approve information in place of a handwritten signature.

4. REQUIREMENTS AND REFERENCES

4.1. DOE O 200.1A, Information Technology Management

4.2. DOE M 200.1-1, Chapter 9, Public Key Cryptography and Key Management

4.3. PS-243-01, Records Management

4.4. PS-563-01, Cyber Security Master Policy, Attachment 10.14 Identification and Authentication (IA) Policy

4.5. PL-240-08, Cyber Security System Security Plan for General Support System

- IA-1 Identification and Authentication Policy and Procedures
- IA-2 User Identification and Authentication

4.6. IMP-8308-03, Software Application Development and Management

4.7. IP-243-03, Identifying, Filing and Maintaining Records

5. DEFINITIONS & ACRONYMS

5.1. Digital Authorization Database: A central relational database containing authorizing data that can be accessed by any authorized relational database and/or application developed and/or maintained by the EMCBC regardless of format.

5.2. Content Owner: The EMCBC Assistant Director responsible for the content and functionality within the given application or system.

5.3. System Owner: The lead individual that has overall responsibility for the implementation for any given application, usually the Assistant Director for Information Resources Management (IRM).

5.4. Developer: IRM staff responsible for coding, testing and placing the application into production.

5.5. Authorizer: An individual given authority or official power to place a written signature on a message or a document, or the approval of data.

5.6. Digital Authorization: Any electronic approval of information or data (e.g. ATAAPS, STRIPES, P-card, ESS, etc.). Digital authorization requires that the identity of the authorizer is authenticated. It also requires security measures to ensure that the information to be conveyed is unchanged after the authorization.

5.7. Hash: A hash algorithm computes a condensed representation of electronic data (message). When a message is input to a hash algorithm, the result is an output called a message digest. Hash algorithms are called secure when, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest (FIPS 180-2).

5.8. Requesting Application: Any relational database and/or application developed and/or maintained by the EMCBC that has been authorized by the Content Owner or System Owner to access the Digital Authorization Database.

6. RESPONSIBILITIES

6.1. Content Owner: Determines which data elements, applications or electronic work processes require implementation of a digital authorization.

6.2. System Owner: Has overall responsibility for implementation of this policy throughout the lifecycle of the application or database.

6.3. Developer: Ensures consistent application of this policy in the development and management of applications and databases designated to utilize a digital authorization.

7. GENERAL INFORMATION

7.1. When paper-based processes are replaced with more efficient electronic workflows and forms, it is important to ensure that authorizations entered electronically have the same integrity as paper signatures.

7.2. Items requiring authorizations will likely become Records, as defined in IP-243-03. Per PS-243-01, Records Management Policy, the IRM AD shall ensure that records management program provisions and standards are included in the scope and planning for all electronic information systems utilized by the EMCBC. Although the EMCBC has selected CA Records Manager (CARM) as its electronic recordkeeping system, it has not yet been fully implemented; thus, any documents generated electronically which become records must be printed and placed in paper recordkeeping files.

7.3. Digital authorizations serve the same purpose as paper signatures, to identify and authenticate the Authorizer and to verify data integrity.

7.4. This policy does not address the use of the Entrust software and the DOE maintained Public Key Infrastructure (PKI), which is used widely within the DOE to attach digital signatures to email and other file based documents. Rather, this policy addresses the need to apply the same principles of digital authorizations to information stored within relational databases and applications developed and/or maintained by the EMCBC.

8. PROCESS

8.1. EMCBC will establish a central Digital Authorization Database that can be accessed by any authorized relational database and/or application developed and/or maintained by the EMCBC regardless of format. The Digital Authorization Database will ensure unique, traceable digital authorizations and shall maintain, at a minimum, the following elements:

8.1.1. Authorizer - Unique information about the Individual Authorizing
8.1.2. Authorizer Role(s) - Defines the limits of the Authorizer authority
8.1.3. Authorization Date - Date that the document was authorized
8.1.4. Serial# - System generated ID for each authorization event
8.1.5. Type of Document - Each application and document utilizing the Digital Authorization Database will be uniquely identified
8.1.6. Authorization Hash - A unique hash of each Authorization request
8.1.7. Authorization Log - A history of Authorization requests

8.2. Content Owner and System Owner will jointly determine which applications and databases require use of the Digital Authorization Database. In general, whenever a work process is automated to include electronic approval in place of handwritten signature, the Digital Authorization Database will be utilized.

8.3. Requesting Applications utilizing the Digital Authorization Database will be configured to:

8.3.1. Capture the network credentials of the Requesting Application's user and system generated date/time to identify the Authorizer and date;
8.3.2. Maintain application security that will only allow Authorizers contained in the Digital Authorization Database to authorize a message, a document, or approve data;
8.3.3. Obtain unique identifying Serial# from the Digital Authorization Database;
8.3.4. Tag the appropriate application database records with the Digital Authorization Database assigned Serial#;
8.3.5. Update the Digital Authorization Database to record the authorization;
8.3.6. Before displaying or reporting signed data, verify that the authorization is still valid by comparing the hash of the document data with the hash value stored in the Digital Authorization Database; and
8.3.7. Produce a signature block on the report or document which includes the following: Signer, Signer Date, Serial # and the notation: "Digitally signed by (to verify contact IRM)".

8.4. The EMCBC will establish routine automated audits to check hash values in the Digital Authorization Database against database values to monitor on-going integrity.

EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.

- Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Original Document	Entire Document	01/17/08
2	Change in Document Numbers	1	09/06/12
	Addition of references	1	
	Addition of CARM as electronic record-keeping system	3	